DEPLOYING MICROSOFT SKYPE FOR BUSINESS OVER FORTINET INTEGRATED WIRELESS

DEPLOYMENT GUIDE

INTRODUCTION

Microsoft Skype for Business provides a UC (Unified Communications) solution at work with instant messaging, online meetings, availability information, and audio and video calling features. Wi-Fi connectivity quality is a critical success factor for UC. This document shows overall network topology, solution components, QoS for Microsoft Skype for Business solution. This best practice guide provides network design considerations for Microsoft's Skype for Business Server and Client over a Fortinet Integrated Wireless network infrastructure.

DEPLOYMENT ARCHITECTURE

This is a typical deployment scenario that provides high-quality calls for the users of the Microsoft Skype for Business. Figure 1 is a typical example of an installation that includes FortiGate as a wireless controller and a Skype for Business.

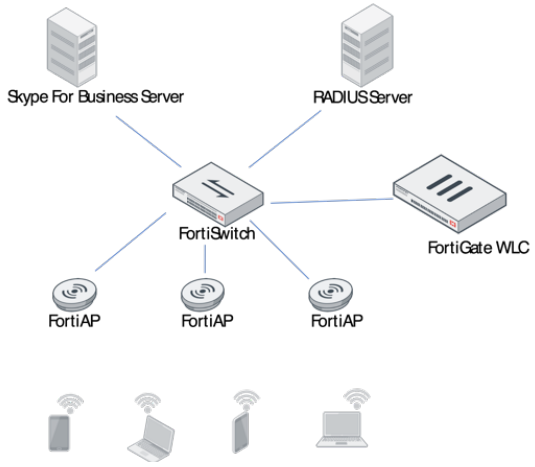

Figure 1

INFRASTRUCTURE COMPONENTS

Skype For Business Server:

Lync Server handles and routes Lync calls between Lync Endpoints.

Skype For Business Client:

Lync Client software could run on Windows or Mac. Lync Client can be initiated video calls or file sharing as UC endpoints.

RADIUS Server

In the enterprise level Wi-Fi network such like WPA2-Enterprise EAP security is recommended. RADIUS server authenticates Wi-Fi users and provides secure and robust Wi-Fi network.

Wi-Fi Controller on FortiGate

The FortiGate, an excellent network security solution, includes wireless controller to secure and manage the Wireless Networks. The web user interface simplifies configuration and administration of the entire WLAN. It provides highly required enterprise security features combined with high availability, enterprise grade wireless features and simple to use interface. FOS v5.6 or above is recommended.

FortiAP

FortiAP supports various Band, Tx Power Control, and channels. FAP v5.6 or above is recommended.

CONFIGURATIONS

The following settings listed below needs to be configured for optimizing Microsoft Skype For Business's user experience.

WIRELESS CONTROLLER ACCESS POINT PROFILE CONFIGURATION

1. Enable OKC (Opportunistic Key Caching). (Enabled by Default)

OKC helps improve client roaming time by reducing the time needed for authentication. Access points (APs) in a network share Pairwise Master Keys (PMKs). By caching PMK, the clients can bypass 802.1X authentication to roam quickly to an AP it has never authenticated to.

```
FG800C-WLAN # config wireless-controller vap
FG800C-WLAN (vap) # edit VAP-FAP
FG800C-WLAN (VAP-FAP) # set okc enable
```

2. Enable Fast Roaming (Enabled by Default)

Fast roaming or BSS Transition (IEEE 802.11r) is an industry standard that reduces the delay due to re-authentication.

```
FG800C-WLAN # config wireless-controller vap
FG800C-WLAN (vap) # edit VAP-FAP
FG800C-WLAN (VAP-FAP) # set fast-roaming enable
```

3. Recommended for Enterprise EAP security for high level security.

Fast roaming or BSS Transition (IEEE 802.11r) is an industry standard that reduces the delay due to re-authentication.

```
FG800C-WLAN # config wireless-controller vap
FG800C-WLAN (vap) # edit VAP-FAP
FG800C-WLAN (VAP-FAP) # show
config wireless-controller vap
   edit "VAP-FAP"
        set vdom "root"
        set ssid "LYNC-ENT"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "RADIUS1"
        set schedule "always"
```

WIRELESS CONTROLLER QoS POLICY CONFIGURATION

WMM setting is based on 802.11e standard to provide QoS to WiFi network. WMM client will classify their traffic in to four Access Classes (AC) such as AC_VO, AC_VI, AC_BE, and AC_BK. DSCP-WMM mapping table is configurable. The below QoS-profile is added audio traffic to be sent at the WMM UP value 6 for Voice, which would most likely carry an Ethernet IP header for DSCP 46 (EF: Expedited Forwarding). The default recommended "WMM enabled" and "WMM-UAPSD enabled" are enabled as default values. 802.11r FT (Fast Transition) roaming is enabled by 'set fast-bss-transition enable'. 802.11k and 802.11v assisted Voice-Enterprise roaming could be enabled by 'set voice-enterprise enable' command. WPA2-Enterprise EAP security level is recommended as high-level security for Voice network. The specific QoS profile is mapped on the access point profile. The command, 'diagnose wireless-controller wlac -c qos-prof', shows all QoS profiles on FortiGate.

```
FG800C-WLAN # config wireless-controller qos-profile
FG800C-WLAN (qos-profile) # edit LYNC-QOS
FG800C-WLAN (LYNC-QOS) # show
config wireless-controller qos-profile
    edit "lync-QOS"
        set dscp-wmm-mapping enable
        set dscp-wmm-vo 48 56 46
        set dscp-wmm-vi 32 40 34
        set dscp-wmm-be 0 24
        set dscp-wmm-bk 8 16

FG800C-WLAN (LYNC-QOS) # get
name                : LYNC-QOS
comment             :
uplink              : 0
downlink            : 0
uplink-sta          : 0
downlink-sta        : 0
burst               : disable
wmm                 : enable
wmm-uapsd           : enable
call-admission-control: disable
dscp-wmm-mapping    : enable
dscp-wmm-vo         : 48 56 46
dscp-wmm-vi         : 32 40 34
dscp-wmm-be         : 0 24
dscp-wmm-bk         : 8 16
FG800C-WLAN (LYNC-QOS) #

FG800C-WLAN # config wireless-controller vap
FG800C-WLAN (vap) # edit LYNC-VAP
FG800C-WLAN (LYNC-VAP) # show
config wireless-controller vap
    edit "LYNC-VAP"
        set vdom "root"
        set ssid "LYNC-ENT"
        set security wpa2-only-enterprise
        set voice-enterprise enable
        set fast-bss-transition enable
        set auth radius
        set radius-server "RADIUS1"
        set schedule "always"
          set qos-profile "LYNC-QOS"
```

```
FG800C-WLAN (LYNC-VAP) # get
name                : LYNC-VAP
vdom                : root
fast-roaming        : enable
external-fast-roaming: disable
max-clients         : 0
ssid                : 4.2.11
broadcast-ssid      : enable
security            : wpa2-only-enterprise
pmf                 : disable
okc                 : enable
voice-enterprise    : enable
fast-bss-transition : enable
radius-mac-auth     : disable
auth                : radius
encrypt             : AES
radius-server       : RADIUS1
acct-interim-interval: 0
intra-vap-privacy   : disable
schedule            : always
ldpc                : rxtx
local-standalone    : disable
local-bridging      : disable
split-tunneling     : disable
vlanid              : 0
dynamic-vlan        : disable
multicast-rate      : 0
multicast-enhance   : disable
broadcast-suppression: dhcp-up arp-known
me-disable-thresh   : 32
probe-resp-suppression: disable
vlan-pooling        : disable
ptk-rekey           : disable
gtk-rekey           : disable
eap-reauth          : disable
qos-profile         : LYNC-QOS
hotspot20-profile   :
rates-11a           :
rates-11bg          :
rates-11n-ss12      :
rates-11n-ss34      :
rates-11ac-ss12     :
rates-11ac-ss34     :
FG800C-WLAN (LYNC-VAP) #
```

SUMMARY

Secure Wi-Fi is critical for a successful implementation of Microsoft Skype for Business unified communications and productivity. Fortinet's Secure Wi-Fi provides an ideal platform for unified communication in the enterprise environment. The best practices listed above have been tested and certified by Microsoft to ensure interoperability and optimized Skype for Business experience.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

153544-0-0-EN January 2, 2018